

OPINIÃO

A nova arquitetura do crime digital

Eduardo Lopes (*)

Nos últimos anos, a dinâmica do crime digital passou por uma transformação profunda.

Se antes era possível associar ataques a indivíduos isolados, muitas vezes trabalhando de forma improvisada, hoje enfrentamos uma verdadeira indústria do cibercrime, organizada em moldes corporativos. Esse modelo inclui hierarquias claras, divisão de funções, investimento constante em ferramentas, uso de tecnologias de ponta e até mesmo processos de recrutamento de especialistas. A consequência imediata se traduz em um ambiente criminoso altamente sofisticado, veloz e resiliente, o que torna os ataques mais difíceis de conter e a resposta das empresas cada vez mais complexa.

Os números confirmam essa evolução. Segundo o relatório “Cenário Global de Ameaças” elaborado pelo laboratório FortiGuard, nos primeiros seis meses de 2025, houve 374 bilhões de tentativas de ataque na América Latina, das quais 84% se concentraram no Brasil. Essa estatística revela não apenas a vulnerabilidade do país, mas também a dimensão global do problema. A velocidade dessas ofensivas é impressionante, já que os criminosos utilizam varreduras automatizadas para identificar falhas de segurança em tempo real, explorando vulnerabilidades antes mesmo de muitas empresas perceberem que elas existem. Quando o ataque é bem-sucedido, as vítimas frequentemente cedem às exigências de pagamento de resgates para retomar suas operações, o que alimenta ainda mais o ciclo de incentivos que mantém esse ecossistema ativo.

Entre as técnicas mais comuns, o roubo de credenciais é o que mais se destaca. Segundo relatório da empresa de segurança cibernética Sophos, aproximadamente 90% dos incidentes confirmados têm origem na quebra de senhas ou logins, um dado que ilustra a fragilidade da identidade digital dos colaboradores. Esse é, atualmente, o alvo preferencial dos criminosos, sobretudo porque credenciais comprometidas podem ser revendidas na deep web e na dark web, espaços digitais clandestinos onde acessos a sistemas corporativos circulam como mercadorias. A ameaça cresce com o uso de ferramentas de Inteligência Artificial treinadas especificamente para fraudes, capazes de criar comunicações falsas quase indistinguíveis das legítimas e automatizar campanhas de ataque em larga escala.

Mais do que investir em ferramentas, as empresas precisam mudar a maneira

como encaram o risco digital. Proteger identidades significa ir além da senha tradicional, incorporando autenticação em múltiplos fatores, revisão contínua dos processos de acesso e a compreensão de que a identidade digital deve ser tratada como o novo perímetro da segurança corporativa. Além disso, monitorar o ambiente externo tornou-se indispensável, já que a visibilidade sobre movimentações em fóruns clandestinos e mercados paralelos pode antecipar incidentes e oferecer sinais de alerta para uma resposta mais ágil.

A tecnologia também desempenha papel essencial na defesa. Ferramentas de automação e inteligência artificial ajudam a reduzir falsos positivos, processar grandes volumes de dados e liberar analistas humanos para atividades que demandam julgamento crítico. Testes constantes de resiliência, como simulações de ataques e exercícios de resposta, são igualmente importantes, porque permitem às equipes aprender na prática e se adaptar à velocidade com que o crime digital evolui. A defesa estática já não atende a um cenário em que o adversário muda de tática a cada nova oportunidade.

No entanto, segurança não deve ser encarada apenas como uma questão técnica. Ela precisa ser discutida em linguagem de negócio, traduzida em impacto financeiro, reputacional e regulatório. Ao compreender que falhas de segurança podem significar desde multas e processos até perda de confiança de clientes e interrupção das operações, os conselhos de administração e a alta liderança tendem a valorizar a área como parte da estratégia de gestão de riscos. Nesse contexto, os investimentos em cibersegurança deixam de ser vistos como despesa e passam a representar proteção de valor e continuidade.

A nova arquitetura do crime digital mostra que o inimigo está mais preparado e organizado do que nunca. Isso exige que empresas também sejam inovadoras em suas defesas, combinando tecnologia, processos e cultura em uma abordagem integrada. Mais do que reagir a incidentes, é preciso construir uma mentalidade preventiva e estratégica. Só assim será possível enfrentar um cenário em que o cibercrime opera em escala global e não dá sinais de retração. Organizações que compreenderem essa realidade e se adaptarem de forma contínua estarão mais bem posicionadas não apenas para sobreviver, mas para garantir resiliência em um ambiente onde a transformação digital e o risco caminham lado a lado.

(*) CEO da Redbelt Security.

Tecnologia e fraudes no pôquer e nas apostas esportivas

O mundo do basquete americano ficou chocado com a recente prisão de Chauncey Billups, um atleta famoso e atual técnico do Portland Trail Blazers, acusado de envolvimento em um sofisticado esquema de fraudes em jogos de pôquer.

Vivaldo José Breternitz (*)

Operação, conduzida pelo FBI, revelou conexões com as famílias mafiosas Gambino, Bonanno, Lucchese e Genovese e o uso de tecnologia avançada para fraudar partidas de pôquer em ambientes privados.

Segundo o FBI, o esquema utilizava dispositivos tecnológicos para fraudar os jogos. Máquinas utilizadas para embaralhar cartas foram modificadas com microcâmeras e sensores ópticos capazes de escanear e registrar a ordem das cartas a serem distribuídas aos jogadores. Essas informações eram transmitidas via rádio ou Wi-Fi a um operador externo, que repassava os dados por diversos meios, como por exemplo, vibrações em smartwatches, a um membro da quadrilha que estava jogando.

Outros recursos utilizados eram a marcação de cartas com tinta visível apenas com o uso de lentes especiais, permitindo aos trapaceiros enxergar as cartas dos adversários. Algumas mesas tinham sensores embutidos que liam as cartas colocadas sobre elas; fichas dotadas de microchips RFID, funcionando como antenas, transmitiam esses dados a um sistema operado pela quadrilha.

Os lucros obtidos eram lavados por meio de criptomoedas e empresas offshore. Billups e outros antigos astros da NBA eram usados como iscas para atrair milionários a essas rodas de pôquer.

No âmbito da mesma operação do FBI, também foram presos Damon Jones, ex-jogador do Cleveland Cavaliers e conhecido por sua ligação com LeBron James e Terry Rozier, jogador do Miami Heat, ambos acusados de passar informações sigilosas sobre atletas, inclusive dados médicos, a envolvidos com apostas.

O escândalo reacende o debate sobre as ligações entre o esporte profissional e o crime organizado, especialmente na área das apostas, que vem se popularizando no Brasil. Também deve



ser lembrada a possibilidade de tecnologia de ponta ser utilizada em fraudes na área de jogos em geral.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjntz@gmail.com.

Empresa brasileira fecha parceria com fornecedora líder de drones VTOL de asa fixa

A Software.com.br, empresa brasileira líder em tecnologia na América Latina, anuncia parceria com a multinacional suíça Wingtra, líder no setor de drones VTOL (decolagem e pouso vertical) de asa fixa que fornece dados aéreos de alta resolução para mapeamento, levantamento e coleta avançada de dados precisos e eficientes para profissionais da indústria geoespacial, como cartógrafos, pesquisadores e especialistas em GIS (Sistemas de Informação Geográfica), que atuam em projetos para os setores de agricultura, mineração, energia, saneamento, construção e em entidades de ensino e pesquisa.

A Software.com.br será responsável pela venda B2B do pacote modular composto pelo drone VTOL de alta precisão WingtraONE e o software WingtraCLOUD no Brasil.

Conhecido por combinar a eficiência de voo de asa fixa com a praticidade de um multirotor (também conhecido como multicóptero – tipo de aeronave com mais de dois rotores geradores de sustentação), o WingtraONE foi projetado para mapeamento aéreo de larga escala, com autonomia para cobrir grandes áreas com precisão centimétrica e com flexibilidade para decolar e pousar em



espaços reduzidos ou de difícil acesso, sem necessidade de pistas de decolagem.

Já o software WingtraCLOUD é uma plataforma baseada em nuvem para planejamento de voos, processamento de fotogrametria RGB. A interface é intuitiva e os fluxos de trabalho automatizados, facilitando o plane-

jamento de missões e o processamento de dados, mesmo para usuários iniciantes. O WingtraCLOUD é compatível com câmeras Infrared e LIDAR e com diversos softwares de pós-processamento de mapeamento, além de oferecer várias ferramentas para melhor atendimento às necessidades de cada negócio.

A comercialização do módulo, reconhecido globalmente para operações confiáveis e seguras, será feita pela Software.com.br por meio de modelo de subscrição com entrega de hardware e software.

“Estamos empolgados com a parceria com a Wingtra, que está na vanguarda do setor de drones e soluções de mapeamento aéreo de alta eficiência e precisão”, afirma Rodrigo Villar, CEO da Software.com.br. “Podemos agora disponibilizar a empresas e instituições dos setores de agricultura, mineração, energia, monitoramento ambiental, segurança, inspeções industriais, busca e resgate e pesquisa, entre outros, o que há de mais avançado em tecnologias de drones que proporcionam resultados consistentes e confiáveis do campo para o escritório, rápida geração de valor e crescimento sustentável baseado em resultados.” (www.software.com.br).

News @TI

ricardosouza@netjen.com.br

Solução inédita de automatização de Departamento Pessoal pode gerar até 40% de economia

A Refuturiza, hub de soluções em educação, tecnologia e empregabilidade, acaba de lançar a Refuturiza DP, uma nova funcionalidade voltada para empresas e departamentos de Recursos Humanos que promete transformar a gestão de pessoas no Brasil. A solução organiza e automatiza toda a rotina do Departamento Pessoal de ponta a ponta, reunindo em um único ambiente recursos como admissão digital, diretório de colaboradores, folha de pagamento, gestão de férias, workflows customizáveis e ponto digital. Diferentemente de outras ferramentas do mercado, que oferecem funcionalidades isoladas, a Refuturiza DP se destaca por integrar todos os processos em um só ecossistema, acessível até mesmo via WhatsApp com apoio de inteligência artificial (www.refuturiza.com.br).

Boxware anuncia acordo comercial com a Avast

A Boxware, empresa com sede em São Paulo e distribuidora de software para revendedores corporativos, anuncia parceria com a Avast, líder em segurança digital e privacidade e parte da Gen, tornando-se distribuidora oficial do Avast Small Business para oferta de soluções completas de segurança cibernética para pequenas empresas em todo o Brasil. Além de ser uma das revendedoras nacionais do Avast Small Business, a parceria inclui suporte individual à rede de canais por meio da gestão de produtos da Boxware, que atuará como especialista técnica em segurança cibernética, incluindo suporte pré-venda, comercial e financeiro. A Boxware também personalizará programas para impulsionar as vendas e gerar novas oportunidades de negócios para as soluções Avast Small Business (https://boxware.com.br/produtos/avast-business/).

Empresas & Negócios José Hamilton Mancuso (1936/2017)

Editorias: Economia/Política: J. L. Lobato (lobato@netjen.com.br); Ciência/Tecnologia: Ricardo Souza (ricardosouza@netjen.com.br); Livros: Ralph Peter (ralphpeter@agenteliterarioralph.com.br); Comercial: comercial@netjen.com.br; Publicidade Legal: lilian@netjen.com.br

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

Laurinda Machado Lobato (1941-2021)

Webmaster/TI: Fabio Nader; Editoração Eletrônica: Ricardo Souza. Revisão: Maria Cecília Camargo; Serviço informativo: Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

ISSN 2595-8410

Responsável: Lilian Mancuso

Jornal Empresas & Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP: 04128-080

Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)

Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90

JUCESP, Nire 35218211731 (6/6/2003)

Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.